Protecting Information in the Post 9/11 World

Safeguards Post 9/11

- Evolving, Heavily Litigated Issue
- Different Types of Information
  - Information may not have been considered as sensitive prior to 9/11
- Classified Information (b)(1)
- Unclassified Information (b)(2) High, (b)(3),

(b)(4), (b)(7)(E), (b)(7)(F)

White House Memorandum

- White House Chief of Staff Andrew Card Memorandum dated March 19, 2002
  - Required agencies to re-examine safeguarding information
  - Scope of review:
    - Chemical, biological, radiological, and nuclear weapons
    - Other sensitive documents related to homeland security

ISOO/OIP Memorandum

- Information Security Oversight Office (ISOO) & Department of Justice, Office of Information and Privacy (OIP) Guidance
  - Exemption 1:
    - Currently classified information
    - Previously unclassified information
    - Previously declassified information

Exemption 1

- Executive Order 12,958, as amended is used to classify information
- New provisions:
  - “Transnational terrorism”--§ 1.4(e) & § 1.4(g)
  - “Infrastructures”--§ 1.4(g)
  - Weapons of mass destruction--§ 1.4(h)

ISOO/OIP Memorandum

- Referenced “sensitive but unclassified information”
- Exemption 1 covers classified information
- Exemptions 2-9 cover unclassified information
- Exemption 2 (High) can be used to protect homeland security types of concerns

Freedom of Information Act

- Exemption 2 applies to information pertaining solely to internal personnel rules and practices of an agency
  - Two parts:
    - **High**: 1. operating rules; guidelines; manuals for investigators, auditors or examiners

      2. examination questions and answers used for training, employment or promotion

      3. computer software, if disclosure would allow circumvention and meets agency record test

FOIA Exemptions

- Exemption 2 (cont'd)
  - **Low**: 1. parking facility rules; lunch hour rules; sick leave policy; file numbers; mail routing stamps; initials; and data processing notations
  - 2. no genuine public interest in this type of information
  - Remember that information must be **internal** to be protected under Exemption 2

(b)(2) High

- Vulnerability studies
  - Schreibman v. U.S. Department of Commerce
  - Vulnerabilities of government systems, programs or installations
    - Cox v. U.S. Department of Justice (1979)
    - Voinche v. FBI (1996)
    - Gordon v. FBI (2005)
    - Poulsen v. U.S. Customs & Border Prot. (2006)

(b)(3)

- Exemption 3 incorporates other federal nondisclosure statutes into the FOIA
- Critical Infrastructure Information (CII)
- Homeland Security Act
  - "covered federal agency" means Department of Homeland Security (DHS)
  - CII must be submitted to DHS
  - This statute only applies to DHS

(b)(4)

- Exemption 4 protects trade secrets and commercial or financial information that is privileged or confidential

- Critical Mass could be used to protect voluntarily submitted information

(b)(4)

- National Parks could be used to protect required submissions

- Question whether there is protection for contractor-supplied homeland security information--not specifically tested in litigation

(b)(7)(E)

- Exemption 7(E) protects techniques and procedures for law enforcement investigations or prosecutions
- Used in conjunction with Exemption 2 (High)
- Can be used to protect homeland security information, but must show law enforcement function--Living Rivers, Inc. v. United States Bureau of Reclamation, 272 F. Supp.2d 1313 (D. Utah 2003)

(b)(7)(F)

- Exemption 7(F) protects law enforcement-related information necessary to protect the physical safety of a wide range of individuals
- Exemption7(F) is playing a bigger role in the FOIA post 9/11
  - L.A. Times Commc'ns, LLC v. Dep't of the Army, 442 F. Supp.2d 880 (C.D. Cal. 2006)
  - Living Rivers, Inc. v. United States Bureau of Reclamation, 272 F. Supp.2d 1313 (D. Utah 2003)